Department of Homeland Security Daily Open Source Infrastructure Report for 30 May 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- TechWeb reports two New York men were arrested in Los Angeles and charged with trying to extort $150,000 from the popular social networking site MySpace.com after allegedly exploiting a service vulnerability that let them steal users' personal information. (See item 12)
- The Associated Press reports New Mexico on Friday, May 26, reported its first death from the plague in 12 years, when a Bernalillo County woman died from septicemic plague. (See item 27)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *May 26, Union Leader (NH)* — **Seabrook nuclear facility gets approval to output more power.** The Nuclear Regulatory Commission (NRC) has granted Seabrook Station, a nuclear facility in Seabrook, NH, an “uprate” in electrical output for the second time in just more than a year. The uprate was approved in two stages; the first uprate of five percent was approved in March 2005, and the second, while approved, will not be implemented until the fall of this year. Between now and then, Seabrook Station’s parent company, Florida Power and Light, will carry out a 30−day shutdown, during which various pieces of equipment will be upgraded, in part to support the uprate. The first expansion of electrical output allowed Seabrook Station to

deliver power to an estimated 70,000 more homes, while the second uprate of 1.7 percent, will mean service to between 15,000 and 17,000 additional residences.
Source: http://www.seacoastonline.com/news/special/5_26special2.htm

2. *May 26, Rutland Herald (VT)* — **Yankee powered down after smoke alarms triggered.** Dust likely caused smoke alarms to go off at Vermont Yankee nuclear power plant Wednesday night, forcing operators to power the facility down and put first−responders in the region on alert, according to the Nuclear Regulatory Commission (NRC). The NRC said Thursday, May 25, that a piece of equipment related to pumping water into the reactor heated up after a motor failure, sending dust into the air and setting off the alarms. The cause of the problem is unknown, the commission said. NRC spokesperson Neil Sheehan said the alarms triggered the carbon dioxide−suppression system in the room and briefly put local and on−site fire and emergency officials on alert. Sheehan said there was no fire or smoke in the room, as initially believed. Sheehan said plant operators followed procedure for pump failures and cut the plant's power production to 57 percent. The plant is now being held at 75 percent power as the cause of the problem is assessed, he said. Vermont Yankee reported the "unusual event" at 9:02 p.m. EST Wednesday, May 24, after what was thought to be smoke or fire set off alarms from the pump motor in the non−nuclear part of the facility.
Source: http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20060526/NEWS/605260345/1003/NEWS02

3. *May 25, Denver Business Journal (CO)* — **Colorado utilities testify before U.S. Senate.** Several Colorado utilities, including Xcel Energy Inc. and Tri−State Generation and Transmission Association told a panel of U.S. senators Thursday, May 25, the nation's major railroad companies are endangering power supplies because they can't reliably deliver coal to burn at power plants. Xcel's David Wilks told the Committee on Energy and Natural Resources that delays in coal deliveries by railroads −− particularly those moving coal from Wyoming's Powder River Basin −− have become so bad that utilities have cut back on burning coal to make electricity and have paid higher prices for natural gas supplies. Some have bought high−priced power on the open market. Utilities say their back−up supplies of coal on the grounds of their plants are dipping lower. Edward Hamberger, of the Association of American Railroads, said traffic out of the Powder River Basin "is back up to normal volumes" and cleaning procedures on the rails are under way.
Source: http://biz.yahoo.com/bizj/060525/1294315.html?.v=1

4. *May 25, U.S. Nuclear Regulatory Commission* — **NRC approves final rule to relieve certain individuals from Energy Act requirements on fingerprinting, criminal history checks.** The U.S. Nuclear Regulatory Commission (NRC) on Thursday, May 25, approved a final rule, immediately effective, to relieve certain individuals who have been approved by the Commission for access to Safeguards Information (SGI) from the fingerprinting and criminal history checks required by the Energy Policy Act of 2005. The regulatory relief, authorized by the Atomic Energy Act, is necessary for the NRC to continue to share SGI with certain categories of international and domestic government representatives. The NRC plans to revise and republish a proposed SGI rule that may more fully address fingerprinting and criminal history checks. SGI is a form of sensitive, unclassified information related to the security of nuclear facilities and materials. Individuals covered by this final rule include federal, state and local officials involved in security planning and incident response, among others. Interrupting

access to this information would impair the NRC's day−to−day implementation of its regulatory programs and hamper communications should an imminent security threat or other emergency occur.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2006/06−0 71.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *May 26, WMICentral (AZ)* — **Hazmat incident in Arizona prompts safety zones, road blocks.** A canister of dichloromethane, about five gallons in size, was found to be leaking in the northwest area of Snowflake, AZ. Once the situation was determined to be hazardous, firefighters cleared a hot zone. Captain Cody Druce stated, "We made sure to expand our safety zones and blocked all travel through the immediate area." Officers were requested to stay in the area in case there were problems at the roadblocks.
Source: http://www.zwire.com/site/news.cfm?newsid=16695398&BRD=2264&PAG=461&dept_id=506181&rfi=6

[Return to top]

Defense Industrial Base Sector

6. *May 25, Washington Technology* — **DoD enlists supercomputers for battle−system testing.** While building body armor prototypes for testing is not overly expensive, building new armored vehicles for testing is just not practical from a cost standpoint. That's where high−performance supercomputers become vitally important to the Department of Defense (DoD) and other agencies. Supercomputers are necessary to run modeling and simulation tests on everything from armor to aircraft wings. As the Army adjusts from a Cold War mind−set to a philosophy of urban warfare, high−speed computing will play an important role in the transition, said Lt. General Joseph Yakovac, military deputy to the assistant secretary of the Army.
Source: http://www.washingtontechnology.com/news/1_1/defense/28636−1 .html

[Return to top]

Banking and Finance Sector

7. *May 26, KHNL−8 (HI)* — **Hawaii's governor signs new laws to fight identity theft.** Hawaii's governor Linda Lingle on Thursday, May 25, signed six bills into law, all designed to consumer information. The bills and their main provisions are as follows: Credit Freeze (HB1871, CD1) allows victims of identity theft to place a security freeze on their credit reports, among other provisions; Security Breach Notification (SB2290, CD1) requires that individuals whose personal information has been compromised by an unauthorized security breach be notified of the breach; Disposal of Personal Information (SB2292, CD1) protects against unauthorized access or use of the information after it is disposed of and ensures that confidential information, when no longer needed, is destroyed; Social Security Number (SSN) Protection (SB2293, CD1)

restricts use of the SSN as an identifier; Confidential Personal Information (SB2159, CD1) makes the act of possessing confidential personal information without proper authorization a criminal offense.
Source: http://www.khnl.com/global/story.asp?s=4952616&ClientType=Pr intable

8. *May 25, Sacramento Business Journal* — **California bank warns of counterfeit dividend checks.** Delta National Bancorp in Manteca, CA, reported to the Federal Deposit Insurance Corp. that counterfeit dividend checks bearing the bank holding company's name are in circulation. The counterfeit items display the routing number assigned to Delta National Bank. The counterfeit items are similar to authentic checks, but the counterfeit paper has a seven−digit account number rather than having eight numbers.
Source: http://www.bizjournals.com/sacramento/stories/2006/05/22/dai ly34.html?from_rss=1

9. *May 25, IDG News Service* — **Phishing pushes e−crime further upstream.** "The Web is under attack," said Phillip Hallam−Baker of VeriSign Inc, who gave a session Thursday, May 25, on Internet crime at the W3C (World Wide Web) conference in Edinburgh, Scotland. The tools to commit e−crime are for sale on the Internet. Mounting an attack on millions of Internet users can be done for a little as U.S. $300, Hallam−Baker said. Networks of computers under the control of hackers, called botnets, can be rented to send spam. Also for sale are lists of up to 100 million e−mail addresses. Hallam−Baker said one Russian hacker will create a custom rootkit −− a method to hide a piece of malicious software deep in a computer's operating system −− for about $60. If users are tricked into clicking on an attachment with a piece of malware, it can mean all of their personal data, such as passwords and credit card numbers, can be recorded and sent back to the hacker, who may resell them to other criminals.
Source: http://www.infoworld.com/article/06/05/25/78676_HNrootofecri me_1.html?source=rss&url=http://www.infoworld.com/article/06 /05/25/78676_HNrootofecrime_1.html

10. *May 25, Copley News Service* — **New Illinois credit law hinders identity theft.** Illinois consumers no longer will have to prove they were victims of identity theft in order to freeze their credit reports under legislation signed by the governor Wednesday, May 24. The new law, which takes effect January 1, also requires a password to remove the freeze. Credit card companies and other lenders commonly use credit reports when considering loan applications. Credit−related complaints, including identity theft, were the second most common complaint received by the Illinois attorney general's office in 2005, after high gasoline prices. Most of the identity−theft complaints resulted from problems with credit cards, mortgages, utilities, and cell phones. The Illinois law includes a $10 fee to implement, lift, or reinstate a credit freeze. The request also would have to be filed with each of the three major credit−reporting agencies.
Source: http://www.saukvalley.com/news/286176659592714.bsp

11. *May 25, CNET News* — **Sacred Heart is latest university to be hacked.** Sacred Heart University in Connecticut is the latest school to be victimized by hackers, according to a message posted on the school's Website. The university said that it discovered the intrusion on Monday, May 8, and notified police and the FBI, which have launched investigations. Sacred Heart offered no details on when the hackers may have entered the system or the kind of information that may have been exposed. Television news channel WTNH reported Thursday, May 25, that the school has notified about 135,000 people that their personal information −−

including Social Security numbers −− may have been compromised. Some of the people notified, according to WTNH's report, have never been associated with Sacred Heart. The news channel quoted an unnamed source who said that the school told him that his name, address, and Social Security number were obtained by the university from information he provided when he took his college entrance exams eight years ago. The report didn't say why Sacred Heart would collect the data, but schools often gather such information for recruiting purposes.
Source: http://news.com.com/Sacred+Heart+is+latest+school+to+be+hacked/2100−7349_3−6077212.html?tag=nefd.top

12. *May 25, TechWeb* — **New York teen pair charged in MySpace extortion plot.** Two New York men were arrested in Los Angeles and charged with trying to extort $150,000 from the popular social networking site MySpace.com, prosecutors announced Wednesday, May 24. The two men allegedly hacked MySpace by exploiting a service vulnerability that let them steal users' personal information. MySpace discovered the intrusion, and notified the joint local and federal task force in Los Angeles. During the investigation, the pair supposedly threatened to release new exploit code unless MySpace came up with $150,000. The two New Yorkers traveled to California Friday, May 19, to meet with MySpace employees, but were met instead by undercover agents from the U.S. Secret Service and the Los Angeles district attorney's office, who arrested them in the sting. Extortion isn't unusual in cyber crime, but it's typically connected with threats to launch a denial−of−service attack against a company's Website. This is one of the first known cases where hackers allegedly threatened to develop exploit code.
Source: http://internetweek.cmp.com/news/188500411;jsessionid=EN5QSJOEX0TI2QSNDBECKICCJUMEKJVN

13. *May 25, VNUNet* — **A quarter of businesses wide open to identity theft, claims report.** Criminals are setting up temporary wireless access points designed to look like the genuine article in order to capture confidential information, according to security firm RSA. The company warned that rogue hotspots could provide the latest platform for identity theft, and cited a test system built by Capgemini UK as a proof−of−concept. "Rogue hotspots currently constitute one of the most serious and most likely vehicles for wireless security breaches...They are easy to set up and an attacker is almost guaranteed a valuable crop of data in a short period of time," said Phil Cracknell of Capgemini UK. RSA warned that rogue hotspots could be used to steal credit card details from transactions made while people were connected. The report suggested that the likelihood of this is relatively high, because a rogue hotspot could allow a higher volume of accurate details to be captured than in an e−mail−based phishing attack. "For this reason, they could be used as the next platform for phishing attacks and identity theft," said Cracknell. RSA also pointed to the fact that almost a quarter of companies with wireless networks in London, Paris, and New York are not secure.
Source: http://www.itweek.co.uk/vnunet/news/2156956/rogue−hotspots−o ffer−biggest

[Return to top]

Transportation and Border Security Sector

14. *May 28, Sunday Mail (Australia)* — **Port terror threat.** Maritime Union of Australia spokesperson Dean Summers said foreign ships carrying explosive cargoes, including ammonium nitrate, were freely sailing Australian waters. "When these ships are issued with a

permit there are no checks of their bona fides," he said. Summers told the Port and Maritime Security and Counter−Terrorism Conference in Sydney that ports and ferries were easy targets for terrorists. "Foreign ships are carrying highly dangerous cargo into our shores, which means our ports and coastal cities are just being laid open to potential terrorists," he said. International security experts have expressed concern al Qaeda's next attack could be maritime. There are fears terrorists may use ships as floating bombs, or hijack a ship and ram it into a port. Summers said it was "a contradiction" that the Federal Government was tightening security of Australian seafarers and port workers while allowing foreign−flagged ships to do whatever they liked.
Source: http://www.thesundaymail.news.com.au/common/story_page/0,5936,19273206%5E903,00.html

15. *May 26, Associated Press* — **Frontier loss widens, CEO predicts profit in current quarter.** The parent company of Frontier Airlines −− the Denver−based low−cost carrier −− reported losses Thursday, May 25, for its latest quarter and fiscal year amid rising fuel costs, but CEO Jeff Potter said he expects the carrier to turn a profit in the current quarter. Frontier Airlines Holdings reported a net loss of $7.9 million, or 22 cents per share, for its fiscal fourth quarter ending March 31, up from a loss of $3.7 million, or 10 cents per share, for the same period a year earlier. Frontier's quarterly results were hurt by fuel costs that rose $17.3 million from the same quarter last year. "If we had the same fuel price this year as we did in last year's quarter, we would actually have a profit," Chief Financial Officer Paul Tate said. Potter said that with strong bookings heading into the summer, Frontier expected to return to profitability in June.
Source: http://www.usatoday.com/travel/flights/2006−05−26−frontier−l oss_x.htm

16. *May 26, Morning Call Online (PA)* — **Air traffic controllers concerned over contract.** Air traffic controllers protested at Pennsylvania's Lehigh Valley International Airport (LVIA) on Thursday, May 25, over a new contract proposed by the Federal Aviation Administration (FAA). Controllers say the new contract would result in cost cuts that could lead to additional retirements. Many airports already have staffing shortages, and the situation could worsen as thousands of controllers approach mandatory retirement age. The FAA has predicted 1,100 people will retire by the end of 2007, and has said it will have adequate staffing levels at all of its airports. LVIA has 26 controllers, including workers in training. The controllers say the airport is authorized to have 30. Many air traffic controllers say shortages have led to increased overtime. Most of the current workers were hired in 1981, after the federal government fired almost all of the existing air traffic controllers because they went on strike. Many are approaching the mandatory retirement age of 56.
Source: http://www.mcall.com/business/local/all−airtrafficcontrolmay26,0,1966606.story?coll=all−businesslocal−hed

17. *May 26, Washington Times* — **Minutemen to start border fence.** The Minuteman Civil Defense Corps (MCDC) will begin construction of new fencing along the U.S.−Mexico border in Palominas, AZ, starting Saturday, May 27. More than 1.15 million illegal aliens were apprehended last year by the Border Patrol, more than half of whom were caught in Arizona. The MCDC, working with Pennsylvania−based WeNeedAFence.com, a grass−roots group that began a campaign last year to construct a secure barrier along the Southwest border, has partnered with six landowners for construction of fencing on their properties and has raised more than $200,000 in donations so far to pay for the project. Surveillance cameras on the

fencing will be monitored via computer by registered Minutemen volunteers across the country, said MCDC President Chris Simcox. The fence's design was the work of WeNeedAFence.com, whose founder, Colin Hanna, described the Arizona project as a "bold and creative private−sector initiative" to bring a secure physical barrier along the nation's southern border. The organization wants separate fences on both sides of the border, each 12− to 15−feet high, separated by a roadway to allow the passage of Border Patrol vehicles.
Source: http://www.washtimes.com/national/20060526−110736−1624r.htm

18. *May 26, Department of Homeland Security* — **Summer 2006 travel season may be busiest on record.** The Memorial Day weekend marks the beginning of the nation's summer travel season. With an estimated 200 million passengers expected to travel by air between the Memorial Day and Labor Day weekends, summer 2006 could be the busiest travel season on record. To help air travelers move smoothly through airport security screening, the Transportation Security Administration (TSA) is offering travel tips and other information on its Website. Information on the TSA Summer Website ranges from wait times at security checkpoints to prohibited items and policies regarding food and beverages.
TSA Summer Website: http://www.tsa.gov/interweb/assetlibrary/summerindex.htm
Source: http://www.dhs.gov/dhspublic/

19. *May 25, USA TODAY* — **Secure border takes serious study.** On a remote campus in Artesia, NM, 482 students are Border Patrol agents−in−training undergoing a rigorous, 19−week course. The Border Patrol Academy prepares men and women to join the rapidly swelling ranks of the agency that polices the nation's porous borders. The number of Border Patrol agents has been growing since the September 11 terrorist attacks. A new academic building with nine 50−seat classrooms has just been completed; a $14 million, 50,000−square−foot addition to the gym is under construction; and new dorms are on the way. On average, 40 people apply for every one accepted at the academy. After three years of steady growth, the Border Patrol is about to embark on an unprecedented expansion. If Congress approves President Bush's request for 6,000 new agents over the next two and one−half years, the patrol will have 18,000 agents on the nation's 5,000 miles of border with Mexico and Canada. That would double the number of agents since 9/11 raised new concerns about terrorists' ability to slip into the country across land borders. Only about 10 percent of all agents are sent to Washington, Michigan, New York, and other states bordering Canada.
Source: http://www.usatoday.com/news/nation/2006−05−25−border−patrol −school_x.htm

20. *May 24, Government Accountability Office* — **GAO−06−801T: National Transportation Safety Board: Preliminary Observations on the Value of Comprehensive Planning, and Greater Use of Leading Practices and the Training Academy (Testimony).** The National Transportation Safety Board (NTSB) is a relatively small agency that plays a vital role in transportation safety and has a worldwide reputation for investigating accidents. With a staff of about 400 and a budget of $76.7 million in fiscal year 2006, NTSB investigates all civil aviation accidents in the United States, and significant accidents in railroad, highway, marine, and pipeline; and issues safety recommendations to address issues identified during accident investigations. To support its mission, NTSB built a training academy, which opened in 2003 and provides training to NTSB investigators and others. It is important that NTSB use its resources efficiently to carry out its mission and maintain its preeminence. This testimony, based on ongoing work for this committee, addresses the extent to which NTSB follows leading

practices in selected management areas, addresses challenges in completing accident investigations and closing safety recommendations, and generates sufficient revenues to cover costs at its academy. Based on completed work to date, the Government Accountability Office (GAO) recommends, among other things, that NTSB develop a revised strategic plan that follows performance−based practices, develop a full cost accounting system, and develop a marketing plan for the academy. NTSB agreed with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d06801thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−801T

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

21. *May 29, Associated Press* — **Tobacco fungal disease found in Kentucky.** A fungus that attacks tobacco plants was found in eastern Kentucky and has already spread, the first reported U.S. outbreak this year, a tobacco specialist said. Blue mold was found on young tobacco plants being raised at two locations in anticipation of spring planting in Magoffin County, said University of Kentucky tobacco pathologist Kenny Seebold. It destroyed two farmers' plants and spread to neighboring Morgan County, he said. Seebold said Friday, May 26, the outbreak occurred about a month earlier than usual in Kentucky, the nation's top producer of burley.
Source: http://www.ohio.com/mld/ohio/business/14692957.htm

22. *May 26, Agricultural Research Service* — **Silencing wheat and barley scab.** A new test to find scab−resistance genes in wheat and barley seed heads uses the plants' natural viral defense mechanism to temporarily "silence" the gene to be tested. The test is an adaptation of a technique called Virus−Induced Gene Silencing (VIGS). Agricultural Research Service (ARS) scientists developed the test with funds from the U.S. Wheat and Barley Scab Initiative. Under the initiative, farmers and scientists work together to combat scab—also known as Fusarium head blight—one of the most devastating wheat and barley diseases worldwide. Currently, there are only a few wheat and barley varieties with effective levels of resistance to scab. The test temporarily incapacitates wheat or barley genes thought to be important to scab resistance, to see if the plant's scab resistance also disappears temporarily. Before this VIGS−based test, there was no way to assess probable genes for scab resistance other than through breeding, or by inserting them into tissue cells and then regenerating whole plants for testing. The new test is much quicker and more efficient since it can be done shortly after a plant is infected with a virus, without waiting to grow a new plant.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

23. *May 26, Stop Soybean Rust News* — **Soybean rust confirmed in Mexican soybean seed−bean fields.** High levels of Asian soybean rust infection recently surprised more than 20 soybean seed growers near Tampico, Mexico. About 650 acres were affected, resulting in

defoliation and potential large yield losses. The soybean rust infections began in January, but became increasingly noticeable in March and April, according to sources from Syngenta. This outbreak was only a short distance south of where Mexican officials reported finding soybean rust in Altamira, also in the State of Tamaulipas. Tamaulipas is the northern−most Mexican state that borders the Gulf of Mexico. Seed beans are generally harvested at the end of April into early May, so the majority of the affected acres should be out of the ground. Mexican growers will begin planting more soybeans closer to the Texas border in late May, for harvest in November.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=825

[Return to top]

Food Sector

24. *May 28, Enid News (OK)* — **Meat recalled.** Advance Food Co. has voluntarily recalled 4.3 million pounds of frozen meat products because they may contain pieces of metal. The meat was sold to institutional buyers nationwide and to one Midwest retail customer with stores in Iowa, Kansas and Missouri. Brian Hayden, vice president of Advance Food, said the company did receive eight consumer complaints about the products produced between March 7 and 18, which were part of a new product line. Hayden said the new product line was produced using a conveyor system and some pieces of meat could have fallen off the conveyor into "catching totes." He said the pieces in the totes inadvertently could have been put back into packaging without being screened by a metal detector.
Food Safety and Inspection Service announcement:
http://www.fsis.usda.gov/PDF/Recall_017_2006_Release.pdf
Source: http://www.enidnews.com/localnews/local_story_148004400.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

25. *May 28, Agence France−Presse* — **Polio vaccination drive in India.** Three−year−old Ashmi Mendiratta was one of the first of 35,000 children to be administered the anti−polio vaccine at an immunization booth in the Indian capital. She was also among the 170 million children targeted by the Indian government in a mammoth immunization program across the country as it struggles to eradicate the disease. The drive, the fourth in five months and set to end Saturday, May 27, "is aimed at ensuring no child below the age of five is left uncovered by the program," said a senior official associated with the initiative. India's health ministry and the World Health Organization's polio program say India has made tremendous progress in curbing the transmission of the crippling disease. India accounted for 83 percent of the world's new polio cases in 2002 with 1,600 cases recorded that year. In India, the number of cases was

brought down to 66 in 2005.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://news.yahoo.com/s/afp/20060528/hl_afp/healthindiapolio_060528224949;_ylt=AsSw0ZazRHeCxiMTF8iEg8GJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA--

26. *May 27, Reuters* — **Decision on smallpox virus destruction delayed.** The World Health Organization (WHO) decided on Saturday, May 27, to defer recommending a new date for destroying the world's last known stockpiles of smallpox. There exists no treatment for the disease that killed millions of people each year into the 1960s and left many more blind and scarred. Smallpox was officially eradicated in 1979 after a worldwide vaccination campaign. The U.S. and Russia, which have since stored the remaining virus samples in high-security laboratories, have long resisted calls to destroy them in case smallpox is found to exist elsewhere. At the WHO's annual assembly, countries were stuck on the text of a resolution aiming to set a date for destroying existing smallpox stocks and to limit tests done on the virus. The WHO will revisit the resolution at an executive board meeting in January. A previous 2002 deadline for destroying smallpox had been waived by the WHO until new vaccines or treatments for smallpox were found.
Source: http://www.alertnet.org/thenews/newsdesk/B594784.htm

27. *May 26, Associated Press* — **New Mexico woman dies from the plague.** New Mexico on Friday, May 26, reported its first death from the plague in 12 years. The state Department of Health confirmed that a Bernalillo County woman died from septicemic plague early last week. The septicemic form occurs when the bacteria multiply in the blood. New Mexico reported four human plague cases last year. There were no human cases in the state in 2004. Plague activity increased last year in Bernalillo County and other areas of north-central New Mexico, a trend that appears to be continuing this year, said Paul Ettestad, public health veterinarian for the Department of Health.
Plague information: http://www.cdc.gov/ncidod/dvbid/plague/index.htm
Source: http://www.washingtonpost.com/wp-dyn/content/article/2006/05/26/AR2006052601994.html

28. *May 26, Associated Press* — **Bird flu kills two siblings in Indonesia.** Preliminary tests have identified two new fatal cases of bird flu in Indonesia, officials said Friday, May 26, as they investigated a separate case involving the largest family cluster ever reported. Indonesia's latest victims, an 18-year-old and his 10-year-old sister from West Java, died Tuesday, May 22, in the state-run Hasan Sidikin hospital in Bandung. Local tests found they were infected by the H5N1 virus, said Nyoman Kandun, head of the Health Ministry's office of communicable disease control.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2006/05/26/AR2006052601011.html

29. *May 26, Agence France-Presse* — **Bird flu spreads to 75 confirmed sites in Romania.** The H5N1 strain of bird flu is spreading in Romania where the number of infected sites rose by 20 to 75, veterinary officials said. In addition, 35 other possible sites were being investigated, the National Veterinary Health Authority said.
Source: http://news.yahoo.com/s/afp/20060526/hl_afp/healthfluromania

_060526202343;_ylt=AkgjGH49UusAwMtB0eINT2GJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

30. *May 27, Pauls Valley Daily Democrat (OK)* — **Bomb hoax prompts review of Oklahoma courthouse evacuation plan.** On May 18, people in the Garvin County Courthouse and others in the nearby vicinity got a real surprise when a bomb threat was made toward the facility in the heart of Pauls Valley, OK. The threat, later deemed a hoax, resulted in county employees and others in the courthouse at the time being forced to scurry out of the building in only a matter of minutes. Although officials saw the overall evacuation as going fairly well, they also know some areas of the procedure will need to be addressed and improvements made when it comes to clearing the courthouse when a real emergency like this one does occur. “We had a drill in December or January and that went perfect,” said Brant Elmore, director of a courthouse security committee. Because of the nature of this particular evacuation, a bomb threat, those leaving the building were soon moved further west of the courthouse. Students in a nearby school were taken to another location. The evacuation itself, which Elmore said took about three to four minutes, was not necessarily an easy thing to accomplish and there is room for improvement.
Source: http://www.paulsvalleydailydemocrat.com/cnhi/paulsvalleydaildemocrat/homepage/local_story_145101658.html?keyword=leadpi cturestory

31. *May 26, Associated Press* — **Rayburn House Office building scare over.** Police briefly sealed off the Capitol Friday, May 26, and launched a floor−by−floor search of the largest office structure on Capitol Hill after an unidentified caller reported gunfire. More than four hours later, police reopened the building. "The search of the Rayburn House Office Building has concluded at this time. The building has reopened for routine business," Capitol Police said, capping a day marked by chaos, confusion and a massive law enforcement deployment. Police said there were no arrests, injuries or confirmation of the gunfire report that had been called in by an unidentified person. The Senate was in session at the time, but the House was not. The Rayburn House Office Building was completed in early 1965 and is the third of three office buildings constructed for the United States House of Representatives. It sits southwest of the Capitol. The building has four stories above ground, two basements, and three levels of underground garage space. Within minutes of the reports, Rayburn halls were virtually empty and police were not allowing anyone to leave or take elevators or stairs to the garage. Incidents of violence inside the Capitol and its office buildings are rare.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=49753

[Return to top]

Emergency Services Sector

32. *May 26, New York Times* — **Flaws in March emergency drill are disclosed.** A simulation that New York City officials held in March to test the ability of city agencies to respond to a deadly

chemical explosion was marred by rescue workers' delays in reaching mock victims and a pileup of official vehicles that thronged the area, officials said Thursday, May 25. The revelations about the March 26 exercise came at a City Council hearing on the Office of Emergency Management's proposed budget. The commissioner of emergency management, Joseph F. Bruno, nevertheless said Thursday that he was "very pleased" with the test of the Citywide Incident Management System, the protocol signed last year that governs how agencies should interact in a big emergency. "We could have probably done a slightly better job in handling the persons who were injured. We saw a real lag in getting people out of the area," said Bruno. Part of the delay resulted from uncertainty about whether and how to move injured victims without more information on the nature and severity of the contamination.
Source: http://www.nytimes.com/2006/05/26/nyregion/26emergency.html?_r=1&oref=slogin

33. *May 26, Beaumont Enterprise (TX)* — **Companies can teach all officials how to plan for hurricane season.** Government officials can learn a lot from the hurricane preparedness plans of retail giant Wal−Mart and San Antonio, TX−based grocer H−E−B. Wal−Mart and H−E−B representatives shared their plans with attendees at the Texas Hurricane Conference Thursday morning, May 25 −− input that some of the state and federal officials at the presentation found impressive. With a command center in Arkansas that watches storms from their infancies in the ocean, Wal−Mart employs the services of professional forecasters to give them the most accurate information possible, along with predicted damages from each storm so they can plan for supplies and manpower as well. And now H−E−B and other stores are entering a joint partnership with the state as primary suppliers for shelters during the storm. As has been the case in the past, the parking lots of such chains will be used as points of distribution for supplies the public needs as well. "There's been a dynamic shift in the realization of the role of the private section," said Jason Jackson, director of emergency management with Wal−Mart. "Federal and state governments are now asking, 'How can we harness the private sector and use them as partners?'"
Source: http://www.southeasttexaslive.com/site/news.cfm?newsid=16696864&BRD=2287&PAG=461&dept_id=512589&rfi=6

34. *May 25, MyWestTexas* — **Law enforcers take class on train crash investigation.** Union Pacific officials held a course for Stanton and Martin County, TX, law enforcers Wednesday, May 24, designed to enhance their aptitude in investigating accidents at railroad crossings. "The program helps with how to go about doing an investigation after a train incident, whether it be a vehicle collision or an event with a pedestrian," said Union Pacific spokesperson Joe Arbona, who explained local police are typically the first responders to rail accidents before the railroad's investigators arrive.
Source: http://www.mywesttexas.com/site/news.cfm?newsid=16690803&BRD=2288&PAG=461&dept_id=475626&rfi=6

[Return to top]

Information Technology and Telecommunications Sector

35. *May 26, Reuters* — **Verizon Wireless passes mark for 911 call location.** Verizon Wireless said on Friday, May 26, more than 95 percent of its customers had phones capable of identifying their location when they call 911 for help. U.S. Federal Communications

Commission regulations required that by the end of last year at least 95 percent of all wireless handsets be able to give emergency personnel the location of a 911 caller. Cingular Wireless and T−Mobile, are using a network−based solution to locate callers that dial 911 for help. Therefore, they were not subject to the 2005 deadline.
Source: http://news.yahoo.com/s/nm/20060526/tc_nm/telecoms_verizonwireless911_dc;_ylt=AlRx8MCndejyL_RyW2QxomcjtBAF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

36. *May 25, Security Focus* — **Symantec Antivirus remote unspecified code execution vulnerability.** Symantec Antivirus is susceptible to an unspecified remote code execution vulnerability. Analysis: A remotely exploitable vulnerability exists within the Symantec Antivirus program. This flaw does not require any end user interaction for exploitation and can compromise affected systems, allowing for the execution of malicious code with SYSTEM level access.
Vulnerable product: Symantec AntiVirus Corporate Edition 10.0.
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18107/references

37. *May 25, Tech Web* — **Windows 2000 bug alert false alarm.** A vulnerability in Windows 2000's file sharing protocol that Symantec rang the alarm on Thursday morning, May 25, is actually not a new bug. Symantec based its warning on a posting to the Dailydave security mailing list. Microsoft countered Symantec's alert: "We've investigated this claim and found the vulnerability being discussed is fixed by MS05−011," wrote Stephen Toulouse, a Microsoft Security Response Center program manager. "What is new is that someone reportedly has found a different way to exploit the vulnerability. But if you have the update, you're protected," added Toulouse.
Microsoft Security Advisory MS05−011:
http://www.microsoft.com/technet/security/bulletin/MS05−011. mspx
Security Focus Advisory: http://www.securityfocus.com/bid/12484/discuss
Source: http://www.techweb.com/wire/security/188500396;jsessionid=FQHJPNXD4TKX0QSNDBCCKH0CJUMEKJVN

38. *May 25, NetworkWorld* — **Telephone excise tax abolished; millions in refunds expected.** The U.S. Department of Treasury abolished a tax law Thursday, May 25, which will likely result in multimillion−dollar refunds for business users. Many business users started filing for refunds as long as three years ago, as the government debated this issue and it was dragged through litigation. The federal excise tax of 3 percent on all long−distance calls has been on the books since 1898, but it is no more. According to the Department of Treasury, the Internal Revenue Service will issue refunds to consumers and business customers for taxes paid over the past three years in their 2006 filings.
Source: http://www.networkworld.com/news/2006/052506−excise−tax.html

39. *May 25, Federal Computer Week* — **DoD: China fielding cyberattack units.** China is stepping up its information warfare and computer network attack capabilities, according to a Department of Defense (DoD) report released last week. The Chinese People’s Liberation Army (PLA) is developing information warfare reserve and militia units and has begun incorporating them into broader exercises and training. Also, China is developing the ability to

launch pre−emptive attacks against enemy computer networks in a crisis, according to the document, “Annual Report to Congress: Military Power of the People’s Republic of China 2006.” The Chinese approach centers on using civilian computer expertise and equipment to enhance PLA operations, the DoD report states.
The referenced report can be found at: http://www.defenselink.mil/pubs/china.html
Source: http://www.fcw.com/article94650−05−25−06−Web

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT continues to receive reports of data theft that targets online users and Federal government web sites. Recently, Veteran Affairs data was stolen from the home computer system of a Veterans Affairs (VA) employee. This data contained large amounts of personally identifiable information, such as, names, social security numbers, and dates of birth. Over 26 million veterans and some spouses are affected by this incident. The VA is continuing to investigate this issue and working to inform affected parties of this incident so that the appropriate steps can be taken to protect against this information being misused. US−CERT recommends that users take the following measures to protect against data theft:

Encrypt sensitive data on your local hard drive and back up mediums.

Attend Security Awareness training to gain a better understanding of your organization's policies and procedures for handling sensitive data.

Restrict access to sensitive data from Internet connected systems.

For additional information, please review the following URL:
http://www.first.gov/veteransinfo

Active Exploitation of a Vulnerability in Microsoft Word

US−CERT is currently researching a zero day vulnerability in Microsoft Word. US−CERT and Microsoft will continue to investigate the public reports to help provide additional guidance as necessary. There is currently no patch available for this vulnerability. For more information please review the following:

Cyber Security Tip: http://www.us−cert.gov/cas/tips/ST04−010.html

Microsoft Security Advisory (919637):
http://www.microsoft.com/technet/security/advisory/919637.ms pxEAF

We will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 32783 (−−−), 25 (smtp), 80 (www), 49200 (−−−), 135 (epmap), 6999 (iatp−normalpri), 113 (auth) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

40. *May 27, Associated Press* — **One dead in Oklahoma City mall shooting.** A young man opened fire in a busy mall Saturday, May 27, injuring a teen before the man was shot and killed by an off−duty sheriff's deputy, authorities said. The shooting occurred around 6:30 p.m. CDT near the entrance to a department store, said Oklahoma County sheriff's spokesperson Mark Myers. The motive for the shooting was not known and there were no other injuries, he said. Sheriff John Whetsel said authorities found no indication of gang involvement during their preliminary investigation. The deputy, who was working as a security guard at the Crossroads Mall, was taking a break when "he heard a commotion downstairs, kind of like a couple of guys fighting, then he heard a gunshot," Myers said. Oklahoma City police have been asked to assist in the investigation into the shooting, Myers said.
Source: http://www.boston.com/news/nation/articles/2006/05/28/1_dead_in_oklahoma_city_mall_shooting/

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer